

CLAIMS

What is claimed is:

1. A method for enabling a firewall to securely pass encrypted data, the method comprising:
 - detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;
 - exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;
 - requesting, based at least in part upon the second security policy, the first encryption key; wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and
 - passing encrypted data when it is determined that the first encryption key is received.

1 2. The method of claim 1, further comprising:

2 not allowing encrypted data to pass when it is
3 determined that the first encryption key is not
4 received.

1 3. The method of claim 1, wherein the step of detecting an
2 exchange of a first encryption key further comprises:

3 monitoring Internet Key Exchange (IKE) protocol data
4 traffic to determine whether the first encryption
5 key is exchanged.

1 4. A method for enabling a firewall to selectively monitor
2 encrypted data traffic, the method comprising:

3 detecting an exchange of a first encryption key between
4 a host device and a remote device, wherein the
5 first encryption key enables confidentiality
6 protection of first data exchanged between the
7 host device and the remote device according to a
8 first security policy;

9 exchanging a second encryption key with the host device
10 when the exchange of the first key is detected,
11 wherein the exchange of the second encryption key
12 enables confidentiality protection of second data

13 exchanged between the firewall and the host device
14 according to a second security policy;
15 requesting, based at least in part upon the second
16 security policy, the first encryption key wherein
17 the first encryption key is sent under the
18 protection of the second encryption key and in
19 accordance with the second security policy; and
20 decrypting encrypted data, using the first encryption
21 key, according to a predetermined monitoring
22 policy.

1 5. A method for enabling a firewall to selectively pass
2 protocols and services, the method comprising:

3 detecting an exchange of a first encryption key between
4 a host device and a remote device, wherein the
5 first encryption key supports confidentiality
6 protection of first data exchanged between the
7 host device and the remote device according to a
8 first security policy;
9 exchanging a second encryption key with the host device
10 when the exchange of the first encryption key is
11 detected, wherein the exchange of the second
12 encryption key supports confidentiality protection
13 of second data exchanged between the firewall and

the host device according to a second security policy;

requesting, based at least in part upon the second security policy, the first encryption key, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy;

decrypting encrypted data, using the first encryption key; and

applying a predetermined filtering policy to the decrypted data.

6. The method of claim 5, further comprising:

re-encrypting the decrypted data.

7. A firewall apparatus that securely passes encrypted data, the apparatus comprising:

an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

a key exchanger for exchanging a second encryption key with the host device when the exchange of the

11 first encryption key is detected, wherein the
12 exchange of the second encryption key supports
13 confidentiality protection of second data
14 exchanged between the firewall and the host device
15 according to a second security policy;
16 a key requestor for requesting, based at least in part
17 upon the second security policy, the first
18 encryption key; wherein the first encryption key
19 is sent under the protection of the second
20 encryption key and in accordance with the second
21 security policy; and
22 an encrypted data passer for passing encrypted data
23 when it is determined that the first encryption
24 key is received.

1 8. The apparatus of claim 7, further comprising:

2 an encrypted data blocker for not allowing encrypted
3 data to pass when it is determined that the first
4 encryption key is not received.

1 9. The apparatus of claim 7, wherein the exchange detector
2 further comprises:

3 a monitor for monitoring Internet Key Exchange (IKE)
4 protocol data traffic to determine whether the
5 first encryption key is exchanged.

1 10. A firewall apparatus for selectively monitoring encrypted

2 data traffic, the apparatus comprising:

3 an exchange detector for detecting an exchange of a
4 first encryption key between a host device and a
5 remote device, wherein the first encryption key
6 enables confidentiality protection of first data
7 exchanged between the host device and the remote
8 device according to a first security policy;

9 a key exchanger for exchanging a second encryption key
10 with the host device when the exchange of the
11 first key is detected, wherein the exchange of the
12 second encryption key enables confidentiality
13 protection of second data exchanged between the
14 firewall and the host device according to a second
15 security policy;

16 a requestor for requesting, based at least in part upon
17 the second security policy, the first encryption
18 key wherein the first encryption key is sent under
19 the protection of the second encryption key and in
20 accordance with the second security policy; and

21 a decryptor for decrypting encrypted data, using the
22 first encryption key, according to a predetermined
23 monitoring policy.

1 11. A firewall apparatus for selectively passing protocols and
2 services, the method comprising:

3 an exchange detector for detecting an exchange of a
4 first encryption key between a host device and a
5 remote device, wherein the first encryption key
6 supports confidentiality protection of first data
7 exchanged between the host device and the remote
8 device according to a first security policy;

9 a key exchanger for exchanging a second encryption key
10 with the host device when the exchange of the
11 first encryption key is detected, wherein the
12 exchange of the second encryption key supports
13 confidentiality protection of second data
14 exchanged between the firewall and the host device
15 according to a second security policy;

16 a requestor for requesting, based at least in part upon
17 the second security policy, the first encryption
18 key, wherein the first encryption key is sent
19 under the protection of the second encryption key
20 and in accordance with the second security policy;

21 a decryptor for decrypting encrypted data, using the
22 first encryption key; and

23 a filter for applying a predetermined filtering policy
24 to the decrypted data.

- 1 12. The apparatus of claim 11, further comprising:
- 2 an encryptor for re-encrypting the decrypted data.